HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10002019-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Richard P. Tarquini
Application No.: 10002,697
Filing Date: October 31, 2001

Confirmation No.: 4671
Examiner: Linh L.D. Son
Group Art Unit: 2135

Title: METHOD, NODE AND COMPUTER READABLE MEDIUM FOR IDENTIFYING DATA IN A NETWORK EXPLOIT

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on June 6, 2006.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120 ☐ 2nd Month $450 ☐ 3rd Month $1020 ☐ 4th Month $1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 500 . At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Label No. EV 568242644US addressed to: Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit: July 7, 2006

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile:

Typed Name: Gail L. Miller

Signature: Gail L. Miller

Respectfully submitted,

Richard P. Tarquini

By Jody C. Bishop

Jody C. Bishop

Attorney/Agent for Applicant(s)

Reg No. : 44,034

Date :

Telephone : (214) 855-8007

08-08-06

TC AF

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Docket No.: 10002019-1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Richard P. Tarquini

Application No.: 10/002,697

Confirmation No.: 4671

Filed: October 31, 2001

Art Unit: 2135

For: METHOD, NODE AND COMPUTER READABLE MEDIUM FOR IDENTIFYING DATA IN A NETWORK EXPLOIT

Examiner: L. L. D. Son

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under § 41.37(a), this brief is filed within two months of the Notice of Appeal filed in this case on June 6, 2006, and is in furtherance of said Notice of Appeal.

The fees required under § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

Hewlett-Packard Development Company, L.P., a Limited Partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249, Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 20 claims pending in application.

B. Current Status of Claims

1. Claims canceled: None
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1-20
4. Claims allowed: None
5. Claims rejected: None

C. Claims On Appeal

The claims on appeal are claims 1-20

IV. STATUS OF AMENDMENTS

A Final Office Action rejecting the claims of the present application was mailed April 6, 2006. In response, Applicant did not file an Amendment After Final Rejection, but instead filed a Notice of Appeal, which this brief supports. Accordingly, the claims on appeal are those as rejected in the Final Office Action of April 6, 2006. A complete listing of the claims is provided in the Claims Appendix hereto.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the separately argued claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. It should be noted that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

According to one claimed embodiment, such as that of independent claim 1, a method of identifying data in a network exploit comprises receiving a packet (e.g., block 235 of FIGURE 9) by an intrusion prevention system (e.g., IPS application 91 of FIGURE 4, driver 147 of FIGURE 6, and *see* page 15, lines 1-18 and page 16, line 21 – page 17, line 31 of the specification) maintained by a node of a network, the intrusion prevention system bound to a media access control driver (e.g., MAC driver 145 of FIGURE 6) and a protocol driver (e.g., protocol driver 135 of FIGURE 6). The method further comprises invoking a signature analysis algorithm by the intrusion prevention system (*see e.g.,* page 8, line 21 of the specification), and utilizing parametric information to select a first rule set (e.g., one of rule sets 200, 201, 202, 203, and 204 of FIGURE 8) from a plurality of rules sets (e.g., rule sets 199-204 of FIGURE 8), the first rule set parametrically related to the packet (*see* page 19, line 6 – page 21, line 4 of the specification). The method further comprises comparing the packet by the intrusion prevention system with the first rule set comprising a rule logically defining a packet signature (*see* blocks 255 and 260 of FIGURE 9, and *see* page 19, line 6 – page 21, line 22 of the specification).

According to another claimed embodiment, such as that of independent claim 7, a node of a network maintaining an instance of an intrusion prevention system for identifying data in a network exploit, where the node comprises a central processing unit (e.g., CPU 272 of FIGURE 4). The node further comprises a memory module (e.g., memory module 274 of FIGURE 4, and *see* page 15, lines 1-18 of the specification) for storing data in machine-readable format for retrieval and execution by the central processing unit. The node further comprises an operating system (e.g., operating system 275 of FIGURE 4) comprising a network stack (e.g., network stack 90 of FIGURE 3) comprising a protocol driver (e.g., protocol driver 135 of FIGURES 3 and 4), a media access control driver (e.g., MAC driver 145 of FIGURES 3 and 4) and an instance of the intrusion prevention system bound to the protocol driver and the media access control driver (e.g., driver 147 of FIGURE 6, and *see* page 15, lines 1-18 and page 16, line 21 – page 17, line 31 of the specification). The intrusion prevention system comprises an associative process engine (e.g., associative process engine 147C of FIGURE 6) and an input/output control layer (e.g., I/O control 147A of FIGURE 6), the input/output control layer operable to receive a signature file generated from a network exploit rule comprising an operand, an operator and a mask, the input/output control layer operable to pass the signature file to the associative process engine (*see* page 16, line 21 – page 19, line 19 of the specification). The associative process engine is operable to utilize parametric information to select the signature file from a plurality of signature files, the signature file parametrically related to a data packet (*see* page 16, line 21 – page 21, line 4 of the specification), and the associative process engine is operable to analyze the data packet with the signature file and assign a logical value to the signature file dependent upon a result from the analysis (*see* page 16, line 21 – page 21, line 4 of the specification).

In certain embodiments, such as that of dependent claim 11, a parametric association is assigned to a subset of the plurality of signature files, and the associative process engine is operable to determine a parametric value of the packet and to analyze the packet with the subset of the signature files when the parametric association of the signature files coincide with the parametric value of the packet (*see* page 16, line 21 – page 21, line 4 of the specification).

In certain embodiments, such as that of dependent claim 13, a plurality of parametric associations are respectively assigned to a plurality of subsets of signature files (*see* page 16, line 21 – page 21, line 4 of the specification).

In certain embodiments, such as that of dependent claim 14, the parametric association is one of a plurality of parametric associations, each of the plurality of parametric associations comprising a common subset of signature files, each signature file of the common subset respectively analyzed by the associative process engine against the network packet prior to analyzation of any other signature files of any other subsets of signature files (*see* page 16, line 21 – page 21, line 4 of the specification).

In certain embodiments, such as that of dependent claim 15, the node further comprises a table (e.g., table of FIGURE 8) maintained in the memory module, the table comprising a plurality of indices each respectively indexing a subset of the plurality of subsets of signature files (*see* page 16, line 21 – page 21, line 4 of the specification).

According to another claimed embodiment, such as that of independent claim 17, a computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of: reading a data packet (e.g., block 235 of FIGURE 9); utilizing parametric information to select a set of a plurality of signature files (e.g., one of sets 200, 201, 202, 203, and 204 of FIGURE 8) from a plurality of sets of signature files (e.g., sets 199-204 of FIGURE 8), the selected set parametrically related to the data packet (*see* page 19, line 6 – page 21, line 4 of the specification), each respective signature file of the plurality of sets of signature files generated from a respective rule of at least one rule set comprised of a plurality of rules; and comparing the data packet with at least one signature file of the selected set (*see* blocks 255 and 260 of FIGURE 9, and *see* page 19, line 6 – page 21, line 22 of the specification).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-6 and 17-20 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,487,666 issued to Shanklin et al. (hereinafter "*Shanklin*").

Claims 7-14 and 16 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Shanklin*.

Claim 15 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Shanklin* in view of U.S. Patent No. 6,279,113 issued to Vaidya (hereinafter "*Vaidya*").

VII. ARGUMENT

Appellant respectfully traverses the outstanding rejections of the pending claims, and requests that the Board reverse the outstanding rejections in light of the remarks contained herein. The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-heading as required by 37 C.F.R. § 41.37(c)(1)(vii).

A. Rejections under 35 U.S.C. §102(e) over *Shanklin*

Claims 1-6 and 17-20 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,487,666 issued to Shanklin et al. (hereinafter "*Shanklin*"). To anticipate a claim under 35 U.S.C. § 102, a single reference must teach each and every element of the claim. *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). As discussed below, *Shanklin* fails to teach each and every element of the claims, and therefore Appellant respectfully requests that the Board overturn these rejections.

<u>Independent Claim 1, and Dependent Claims 2-6</u>

Independent claim 1 recites:

> A method of identifying data in a network exploit, comprising:
> receiving a packet by an intrusion prevention system maintained by a node of a network, the intrusion prevention system bound to a media access control driver and a protocol driver;

> invoking a signature analysis algorithm by the intrusion prevention system;
>
> <u>utilizing parametric information to select a first rule set from a plurality of rules sets, the first rule set parametrically related to the packet</u>; and
>
> comparing the packet by the intrusion prevention system with the first rule set comprising a rule logically defining a packet signature. (Emphasis added).

Shanklin fails to teach at least the above-emphasized element of independent claim 1. That is, as discussed further below, *Shanklin* fails to teach utilizing parametric information to select from a plurality of rule sets a first rule set that is parametrically related to a received packet. *Shanklin* provides no such teaching of selecting a first rule set of a plurality of rule sets, but rather appears to teach simply analyzing all defined rule sets against a received packet, as discussed further herein.

Shanklin is directed to a "method of describing intrusion signatures, which are used by an intrusion detection system to detect attacks on a local network." Abstract of *Shanklin*. In summary, *Shanklin* provides (at col. 2, lines 3-21):

> One aspect of the invention is a method of describing signatures used for detecting intrusion to a local network. The method combines features of both regular expression methodology and logical expression methodology. A set of regular expression identifiers is used to represent a set of "signature events". A "signature event" may be a packet type, a sequence of packet types, or any one of a number of signature-related events, such as a count or a time period. Logical operators are used to describe relationships between the signature events, such as whether a count exceeds a certain value. For each signature, one or more of these identifiers and operators are combined to provide a regular expression describing that signature.
>
> An advantage of the invention is that it provides an abstraction for describing intrusion signatures. The signatures are written in a descriptive language rather than in procedural computer code. Security technicians who work with local networks need not learn a programming language in order to describe signatures.

While *Shanklin* appears to provide rules for use in analyzing received packets for detecting intrusions, *Shanklin* provides no teaching of utilizing parametric information to select from a plurality of rule sets a first rule set that is parametrically related to a received packet. In the Final Office Action, the Examiner asserts that *Shanklin* teaches this feature, citing to col. 3, lines 48-53, col. 4, lines 30-33, col. 5, lines 12-18, and col. 5, lines 35-48 of *Shanklin*, *see* page 11 of the Final Office Action. Each of the cited portions of *Shanklin* are

produced below for the Board's convenience, and Appellant addresses each cited portion.

First, col. 3, lines 48-53 of *Shanklin* provides:

> Router 12 decides whether to forward a packet by examining the packet's protocol level addresses. Router 12 is capable of handling any datalink protocol, thus, ethernet, FDDI, ISDN, and so on are handled in the same manner.

This portion of *Shanklin* merely describes that a router is operable to examine a packet's protocol level address for forwarding the packet appropriately. This is merely the normal operation of a router, and does not provide any teaching whatsoever of selecting a rule set that is parametrically related to a received packet.

Next, col. 4, lines 30-33 of *Shanklin* provides:

> Signatures may also be categorized as being either atomic or composite. Atomic signatures comprise information (context or content) in a single packet. Composite signatures comprise information in multiple packets.

This portion of *Shanklin* merely mentions that signatures may be atomic or composite. Again, this portion of *Shanklin* does not provide any teaching whatsoever of selecting a rule set that is parametrically related to a received packet.

Col. 5, lines 12-18 of *Shanklin* provides:

> As applied to signature detection analysis, each type of packet associated with a signature can be described with a unique identifier. A regular expression having identifiers of this type is referred to herein as a "packet-based" regular expression. A packet-based regular expression might have the following form: "C.*CC[^C]C
> where C is a defined packet type. Thus, instead of C representing a character as is the case with conventional regular expressions, C represents a packet type.

Thus, the above portion of *Shanklin* appears to teach that a packet type can be represented in an expression that is used in signature analysis. In other words, *Shanklin* appears to teach that "packet type" can be used as an expression in a rule that is used for performing signature analysis to detect intrusions. However, this portion of *Shanklin* does not provide any teaching whatsoever of selecting a rule set that is parametrically related to a

received packet. While "packet type" may be used in defining a rule that is used for intrusion detection in *Shanklin*, no such parametric information is used in *Shanklin* for selecting from a plurality of rule sets a first rule set that is parametrically related to a received packet. Again, no such selection of a first rule set from a plurality of rule sets is mentioned at all in the above portion of *Shanklin*, but rather the above portion of *Shanklin* appears to merely provide that an expression of "packet type" may be used in a rule.

Finally, col. 5, lines 35-48 of *Shanklin* provides:

> The use of regular expressions can be extended so that each identifier represents an "event", which could be a single packet, a sequence of packets, or a signature-related event. A signature-related event could be, or could include, a time period, a count, a packet in the opposing direction, or any other conceivable event that could be part of a signature. This type of regular expression is referred to herein as an "event-based" regular expression.
>
> Because signatures often comprise events as well as packets types, the use of regular expression methodology can be combined with logical expression (Boolean) methodology to more completely describe signatures. Logical expressions involve the use of operators that relate parts of an expression so that the outcome is true or false. Logical operators include AND, OR, NOT, and greater than, less than, or equal to.

Thus, the above portion of *Shanklin* appears to teach that regular expressions (or "rules") may be defined using Boolean operators. However, this portion of *Shanklin* does not provide any teaching whatsoever of selecting a rule set that is parametrically related to a received packet. While rules may be defined (as regular expressions) in *Shanklin*, *Shanklin* provides no teaching of utilizing parametric information for selecting from a plurality of rule sets a first rule set that is parametrically related to a received packet. Again, no such selection of a first rule set from a plurality of rule sets is mentioned at all in the above portion of *Shanklin*, but rather the above portion of *Shanklin* appears to merely provide that rules may be defined as regular expressions using Boolean operators.

In view of the above, the cited portions of *Shanklin* relied upon by the Final Office Action fail to teach utilizing parametric information to select a first rule set from a plurality of rules sets, the first rule set parametrically related to the packet, as recited by claim 1. Further, no other portion of *Shanklin* teaches this element. Again, while *Shanklin* appears to teach defining rules (as regular expressions) for comparison with packets in detecting intrusions, *Shanklin* provides no teaching of utilizing parametric information to select from a

plurality of rule sets a first rule set that is parametrically related to a received packet.

Rather, *Shanklin* appears to suggest that all defined rules are analyzed against all received packets, and provides no teaching whatsoever of utilizing parametric information for selecting a first rule set of a plurality of rule sets to compare with a received packet. The present application explains, at page 19, lines 6-19, for example, that such utilization of parametric information for selecting a rule set to compare against a received packet allows the intrusion detection system to avoid analyzing the received packet against signatures that are parametrically unrelated thereto. For instance, a rule set containing rules defining signatures that are applicable only to UDP packets need not be analyzed for a non-UDP packet. *Shanklin* fails to provide any teaching whatsoever of utilizing parametric information for selecting one of a plurality of rule sets to compare with a received packet, but instead appears to teach that all of its defined rules are compared against all received packets. A given rule itself may contain an expression (e.g., packet type) that is determined during the analysis of the rule against the received packet as not applying to such packet, but *Shanklin* provides no teaching of avoiding such analysis of the given rule by selecting a rule set that is parametrically related to the received packet.

In view of the above, *Shanklin* fails to teach all elements of claim 1. Therefore, Appellant respectfully requests that the Board overturn the rejection of claim 1.

Also, dependent claims 2-6 depend either directly or indirectly from claim 1, thus inheriting all of the limitations of independent claim 1. As noted above, *Shanklin* does not teach every element of independent claim 1. Consequently, *Shanklin* also fails to teach every element of dependent claims 2-6. Therefore, Appellant respectfully requests that the Board overturn the rejection of claims 2-6.

<u>Independent Claim 17 and Dependent Claims 18-20</u>

Independent claim 17 recites:

> A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:
> reading a data packet;

> utilizing parametric information to select a set of a plurality of signature files from a plurality of sets of signature files, the selected set parametrically related to the data packet, each respective signature file of the plurality of sets of signature files generated from a respective rule of at least one rule set comprised of a plurality of rules; and
>
> comparing the data packet with at least one signature file of the selected set. (Emphasis added).

Shanklin fails to teach at least the above-emphasized element of claim 17. As discussed above with claim 1, *Shanklin* fails to teach utilizing parametric information to select a set of a plurality of signature files that is related to a received data packet. While *Shanklin* allows for rules to be defined for use in performing signature analysis on a received packet, *Shanklin* provides no teaching of utilizing parametric information to select a set of signature files that a parametrically related to a received data packet for use in comparison with the data packet. Rather, *Shanklin* appears to teach comparing all of its rules (signature files) against each received packet, and does not select a set of the signature files that are parametrically related to the data packet for such comparison.

In view of the above, *Shanklin* fails to teach all elements of claim 17. Therefore, Appellant respectfully requests that the Board overturn the rejection of claim 17.

Also, dependent claims 18-20 depend either directly or indirectly from claim 17, thus inheriting all of the limitations of independent claim 17. As noted above, *Shanklin* does not teach every element of independent claim 17. Consequently, *Shanklin* also fails to teach every element of dependent claims 18-20. Therefore, Appellant respectfully requests that the Board overturn the rejection of claims 18-20.

B. Rejections Under §103(a) over *Shanklin*

Claims 7-14 and 16 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *Shanklin.* Appellant respectfully traverses these rejections below.

To establish a prima facie case of obviousness, three basic criteria must be met. *See* M.P.E.P. § 2143. First, there must be some suggestion or motivation, either in the applied references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the applied references must teach or suggest all

the claim limitations. Without conceding any other criteria, Appellant respectfully asserts that *Shanklin* fails to teach or suggest all of the claim limitations, as discussed further below.

Independent Claim 7 and Dependent Claims 8-10 and 16

Independent claim 7 recites:

> A node of a network maintaining an instance of an intrusion prevention system for identifying data in a network exploit, the node comprising:
> a central processing unit;
> a memory module for storing data in machine-readable format for retrieval and execution by the central processing unit; and
> an operating system comprising a network stack comprising a protocol driver, a media access control driver and an instance of the intrusion prevention system bound to the protocol driver and the media access control driver, the intrusion prevention system comprising an associative process engine and an input/output control layer, the input/output control layer operable to receive a signature file generated from a network exploit rule comprising an operand, an operator and a mask, the input/output control layer operable to pass the signature file to the associative process engine, the associative process engine operable to utilize parametric information to select the signature file from a plurality of signature files, the signature file parametrically related to a data packet, the associative process engine operable to analyze the data packet with the signature file and assign a logical value to the signature file dependent upon a result from the analysis. (Emphasis added).

Shanklin fails to teach or suggest at least the above-emphasized element of claim 7. That is, *Shanklin* fails to teach or suggest an operating system comprising an instance of an intrusion prevention system that comprises an associative process engine as recited by claim 7. *Shanklin* provides no teaching or suggestion of an associative process engine that is operable to utilize parametric information to select from a plurality of signature files a signature file that is parametrically related to a data packet.

As discussed above with claim 1, *Shanklin* fails to teach utilizing parametric information to select from a plurality of signature files a signature file that is parametrically related to a received data packet. While *Shanklin* allows for rules to be defined for use in performing signature analysis on a received packet, *Shanklin* provides no teaching of selecting a signature file that is parametrically related to a received data packet for use in analyzing the data packet against the selected signature file. Rather, *Shanklin* appears to

teach analyzing all of its rules (signature files) against each received packet, and does not teach or suggest an associative process engine as recited by claim 7.

In view of the above, *Shanklin* fails to teach or suggest all elements of claim 7. Therefore, Appellant respectfully requests that the Board overturn the rejection of claim 7.

Also, dependent claims 8-10 and 16 depend either directly or indirectly from claim 7, thus inheriting all of the limitations of independent claim 7. As noted above, *Shanklin* does not teach or suggest every element of independent claim 7. Consequently, *Shanklin* also fails to teach or suggest every element of dependent claims 8-10 and 16. Therefore, Appellant respectfully requests that the Board overturn the rejection of claims 8-10 and 16.

Dependent Claims 11 and 12

Dependent claim 11 depends indirectly from independent claim 7, and thus includes all of the limitations of claim 7 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 11 is allowable at least because of its dependence from claim 7 for the reasons discussed above.

Claim 11 further recites "wherein a parametric association is assigned to a subset of the plurality of signature files, the associative process engine operable to determine a parametric value of the packet and to analyze the packet with the subset of the signature files when the parametric association of the signature files coincide with the parametric value of the packet." *Shanklin* fails to teach or suggest a parametric association being assigned to a subset of a plurality of signature files. *Shanklin* further fails to teach or suggest an associative process engine that is operable to determine a parametric value of a packet and determine whether the parametric association of a signature file coincides with the parametric value of the packet.

Thus, for this further reason, *Shanklin* fails to teach or suggest all elements of claim 11. Therefore, the rejection of claim 11 should be overturned.

Dependent claim 12 depends from claim 11, and thus inherits all elements of claim 11, as well as all elements of independent claim 7 from which claim 11 depends. Thus, claim 12 is allowable over *Shanklin* at least for the reasons discussed above with claims 7 and 11.

Dependent Claim 13

Dependent claim 13 depends from claim 11, which depends indirectly from independent claim 7, and thus claim 13 includes all of the limitations of claims 7 and 11 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 13 is allowable at least because of its dependence from claims 7 and 11 for the reasons discussed above.

Claim 13 further recites "wherein a plurality of parametric associations are respectively assigned to a plurality of subsets of signature files." *Shanklin* fails to teach or suggest assigning a respective parametric association to a plurality of subsets of signature files. Subsets of the signature files of *Shanklin* are not assigned a respective parametric association. Rather, the signature files of *Shanklin* are not so categorized.

Thus, for this further reason, *Shanklin* fails to teach or suggest all elements of claim 13. Therefore, the rejection of claim 13 should be overturned.

Dependent Claim 14

Dependent claim 14 depends from claim 11, which depends indirectly from independent claim 7, and thus claim 14 includes all of the limitations of claims 7 and 11 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 14 is allowable at least because of its dependence from claims 7 and 11 for the reasons discussed above.

Claim 14 further recites "wherein the parametric association is one of a plurality of parametric associations, each of the plurality of parametric associations comprising a common subset of signature files, each signature file of the common subset respectively analyzed by the associative process engine against the network packet prior to analyzation of any other signature files of any other subsets of signature files." *Shanklin* fails to teach or suggest this further element of claim 14. Again, *Shanklin* provides no associative process engine that analyzes parametric association of a signature file.

Thus, for this further reason, *Shanklin* fails to teach or suggest all elements of claim 14. Therefore, the rejection of claim 14 should be overturned.

C. Rejection Under §103(a) over *Shanklin* in view of *Vaidya*

Claim 15 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Shanklin* in view of U.S. Patent No. 6,279,113 issued to Vaidya (hereinafter "*Vaidya*"). Appellant respectfully traverses these rejections below.

To establish a prima facie case of obviousness, three basic criteria must be met. *See* M.P.E.P. § 2143. First, there must be some suggestion or motivation, either in the applied references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the applied references must teach or suggest all the claim limitations. Without conceding any other criteria, Appellant respectfully asserts that the applied combination of *Shanklin* and *Vaidya* fails to teach or suggest all of the claim limitations, as discussed below.

Claim 15 depends indirectly from independent claim 7, and thus inherits all of the limitations of claim 7 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 15 is allowable at least because of its dependence from claim 7 for the reasons discussed above, as the Examiner does not rely upon *Vaidya* as curing the above-noted deficiencies in *Shanklin* with respect to claim 7, nor does *Vaidya* do so.

Claim 15 further recites "a table maintained in the memory module, the table comprising a plurality of indices each respectively indexing a subset of the plurality of subsets of signature files." The Final Office Action concedes at page 10 thereof that *Shanklin* fails to teach or suggest this further element of claim 15. However, the Final Office Action asserts that *Vaidya* teaches the recited table. Appellant respectfully disagrees. *Vaidya* fails to teach or suggest a table comprising a plurality of indices each respectively indexing a subset of a plurality of subsets of signature files. Rather, *Vaidya* merely mentions a database to which signature files are stored, and provides no teaching or suggestion of index respective subsets of signature files, as recited by claim 15.

In asserting that *Vaidya* teaches such a table that indexes a subset of a plurality of subsets of signature files, the Examiner cites to Col. 2, lines 30-45 of *Vaidya*. The cited portion of *Vaidya* provides:

> A static signature database intrusion detection system (IDS) overcomes some of the above described limitations by providing a static signature database engine which includes a set of attack signature processing functions, each of which is configured to detect a specific intrusion type. Each attack signature is descriptive of a pattern which constitutes a known security violation. The system monitors network traffic by sequentially executing every processing function of a database engine for each data packet received over a network. Each processing function of the database engine is integrally associated with a corresponding attack signature making it problematic to incorporate new attack signatures into an existing static signature database. An entirely new database engine must be constructed in order to incorporate a new attack signature. This limitation also results in the built-in IDS not being able to allow addition and customization of new signatures. Furthermore, a built-in database IDS suffers from performance loss due to the sequential execution of every processing function for each packet received over the network. The IDS performance degrades further as more signatures are added to the database engine because of the resulting delay caused by the sequential processing by the static database engine.

As can be seen above, the cited portion of *Vaidya* merely mentions storing signatures to a database, and makes no mention whatsoever of indexing respective subsets of signature files, as recited by claim 15. Thus, for this further reason, the combination of *Shanklin* and *Vaidya* fails to teach or suggest all elements of claim 15. Therefore, the rejection of claim 15 should be overturned.

D. Conclusion

In view of the above, Appellant requests that the board overturn the outstanding rejections of claims 1-20. Attached hereto are a Claims Appendix, Evidence Appendix, and Related Proceedings Appendix. As noted in the attached Evidence Appendix, no evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted. Also, as noted by the Related Proceedings Appendix, no related proceedings are referenced in II above, and thus no copies of decisions in related proceedings are provided.

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Label No. EV 568242644US in an envelope addressed to: M/S Appeal Brief-Patents, Commissioner for Patents, Alexandria, VA 22313.

Date of Deposit: August 7, 2006

Typed Name: Gail L. Miller

Signature: Gail L. Miller

Respectfully submitted,

By: Jody C. Bishop
Jody C. Bishop
Attorney/Agent for Applicant(s)
Reg. No. 44,034
Date: August 7, 2006
Telephone No. (214) 855-8007

VIII. CLAIMS APPENDIX

Claims Involved in the Appeal of Application Serial No. 10/002,697

1. A method of identifying data in a network exploit, comprising:

receiving a packet by an intrusion prevention system maintained by a node of a network, the intrusion prevention system bound to a media access control driver and a protocol driver;

invoking a signature analysis algorithm by the intrusion prevention system;

utilizing parametric information to select a first rule set from a plurality of rules sets, the first rule set parametrically related to the packet; and

comparing the packet by the intrusion prevention system with the first rule set comprising a rule logically defining a packet signature.

2. The method according to claim 1, wherein receiving a packet by an intrusion prevention system further comprises receiving a packet originating from the node.

3. The method according to claim 1, wherein receiving a packet by an intrusion prevention system further comprises receiving a packet originating from a source external to the node, the packet addressed to the node.

4. The method according to claim 1, further comprising discarding the packet upon determination that a signature of the packet corresponds to the rule.

5. The method according to claim 1, wherein comparing the packet by an intrusion prevention system with a first rule set further comprises comparing the packet by the intrusion prevention system with a second rule set upon determination that a signature of the packet does not correspond to a rule of the first rule set.

6. The method according to claim 1, wherein comparing the packet by the intrusion prevention system with a first rule set further comprises comparing the packet by the intrusion prevention system with a rule set comprising a plurality of rules each respectively comprising machine-readable code logically defining a packet signature.

7. A node of a network maintaining an instance of an intrusion prevention system for identifying data in a network exploit, the node comprising:

a central processing unit;

a memory module for storing data in machine-readable format for retrieval and execution by the central processing unit; and

an operating system comprising a network stack comprising a protocol driver, a media access control driver and an instance of the intrusion prevention system bound to the protocol driver and the media access control driver, the intrusion prevention system comprising an associative process engine and an input/output control layer, the input/output control layer operable to receive a signature file generated from a network exploit rule comprising an operand, an operator and a mask, the input/output control layer operable to pass the signature file to the associative process engine, the associative process engine operable to utilize parametric information to select the signature file from a plurality of signature files, the signature file parametrically related to a data packet, the associative process engine operable to analyze the data packet with the signature file and assign a logical value to the signature file dependent upon a result from the analysis.

8. The node according to claim 7, wherein the exploit rule further comprises a composite of a plurality of rules, each rule comprising an operand, an operator and a mask and having a logical value, each of the plurality of rules being logically connected with at least one of the other plurality of rules by a non-bitwise boolean operator, the logical value of the signature file dependent on the logical value of each of the plurality of rules.

9. The node according to claim 7, wherein the operand comprises network frame data, the operator comprises a bitwise operation, and the mask comprises an operator mask.

10. The node according to claim 7, wherein the network control layer is operable to receive the plurality of signature files each respectively generated from a network exploit rule.

11. The node according to claim 10, wherein a parametric association is assigned to a subset of the plurality of signature files, the associative process engine operable to determine a parametric value of the packet and to analyze the packet with the subset of the signature files when the parametric association of the signature files coincide with the parametric value of the packet.

12. The node according to claim 11, wherein the parametric value of the packet is obtained from link-layer header information of the packet.

13. The node according to claim 11, wherein a plurality of parametric associations are respectively assigned to a plurality of subsets of signature files.

14. The node according to claim 11, wherein the parametric association is one of a plurality of parametric associations, each of the plurality of parametric associations comprising a common subset of signature files, each signature file of the common subset respectively analyzed by the associative process engine against the network packet prior to analyzation of any other signature files of any other subsets of signature files.

15. The node according to claim 10, further comprising a table maintained in the memory module, the table comprising a plurality of indices each respectively indexing a subset of the plurality of subsets of signature files.

16. The node according to claim 7, wherein the intrusion prevention system further comprises an intrusion event manager, the associative process engine operable to communicate that the analysis of the packet indicates a correspondence with the signature file, the intrusion event manager operable to generate an alert that is transmitted from the node to at least one of a management node in a network and an event database maintained by the node.

17. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

reading a data packet;

utilizing parametric information to select a set of a plurality of signature files from a plurality of sets of signature files, the selected set parametrically related to the data packet, each respective signature file of the plurality of sets of signature files generated from a respective rule of at least one rule set comprised of a plurality of rules; and

comparing the data packet with at least one signature file of the selected set.

18. The computer readable medium according to claim 17, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of determining whether a correspondence between a signature of the data packet and the at least one signature files exists.

19. The computer readable medium according to claim 17, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of comparing the data packet with each signature file of the selected set of the plurality of signature files.

20. The computer readable medium according to claim 19, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of:

upon determining that no correspondence exists between the signature of the data packet and the signature files of the selected set of the plurality of signature files, selecting a second set of signature files from the plurality of sets of signature files; and

comparing the signature of the data packet to at least one signature file of the second set of signature files.

IX. EVIDENCE APPENDIX

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

X. RELATED PROCEEDINGS APPENDIX

No related proceedings are referenced in II above, and thus no copies of decisions in related proceedings are provided.